

2 セットアップ

本体の設置からお使いなれる状態にするまでの手順について説明します。また、装置を再セットアップする場合もここに記載している説明を参照してください。

設置と接続

本体の設置と接続について説明します。

設　置

本装置は卓上またはEIA規格に適合したラックに設置して使用します。

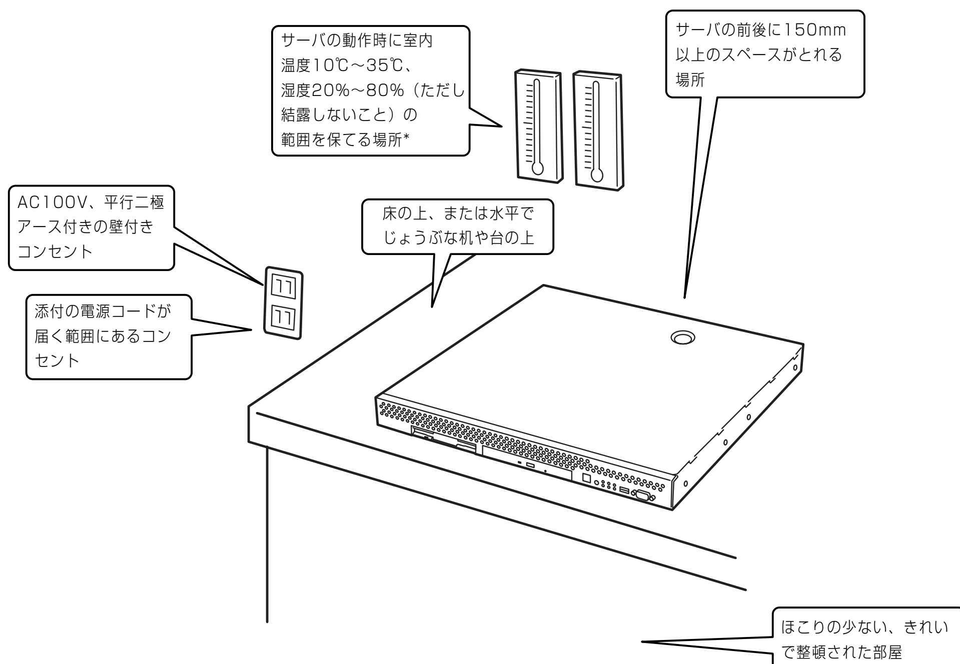
卓上への設置

⚠ 注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指定以外の場所に設置しない**

本体の設置にふさわしい場所は次のとおりです。

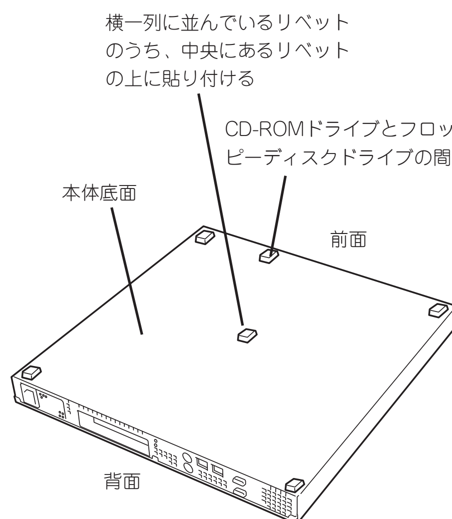


* 室内温度15℃～25℃の範囲を保てる場所での使用をお勧めします。

次に示す条件に当てはまるような場所には、設置しないでください。これらの場所に本装置を設置すると、誤動作の原因となります。

- 温度変化の激しい場所(暖房器、エアコン、冷蔵庫などの近く)。
- 強い振動の発生する場所。
- 腐食性ガスの発生する場所、薬品類の近くや薬品類がかかるおそれのある場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。
- 電源コードまたはインタフェースケーブルを足で踏んだり、引っ掛けたりするおそれのある場所。
- 強い磁界を発生させるもの(テレビ、ラジオ、放送/通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本装置の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどでON/OFFする場合の接点スパークなど)を発生する装置の近くには設置しないでください。(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください。)

卓上に置く場合は、本体底面に添付のゴム足を貼り付けてください。
設置場所が決まったら、本体の底面をしっかりと持って、設置場所にゆっくりと静かに置いてください。本装置は3台まで積み重ねて置くことができます。



ラックへの設置

ラックの設置については、ラックに添付の説明書を参照するか、保守サービス会社にお問い合わせください。
ラックの設置作業は保守サービス会社に依頼することもできます。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指定以外の場所で使用しない**
- **アース線をガス管につながない**

⚠注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **一人で搬送・設置をしない**
- **一人で部品の取り付けをしない**
- **荷重が集中してしまうような設置はしない**
- **ラックが不安定な状態でデバイスをラックから引き出さない**
- **複数台のデバイスをラックから引き出した状態にしない**
- **定格電源を超える配線をしない**

次に示す条件に当てはまるような場所には、ラックを設置しないでください。これらの場所にラックを設置したり、ラックに本装置を搭載したりすると、誤動作の原因となります。

- 装置をラックから完全に引き出せないような狭い場所。
- ラックや搭載する装置の総質量に耐えられない場所。
- スタビライザが設置できない場所や耐震工事を施さないと設置できない場所。
- 床におうとつや傾斜がある場所。
- 温度変化の激しい場所(暖房器、エアコン、冷蔵庫などの近く)。
- 強い振動の発生する場所。
- 腐食性ガスの発生する場所、薬品類の近くや薬品類がかかるおそれのある場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。

- 強い磁界を発生させるもの(テレビ、ラジオ、放送/通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本装置の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどでON/OFFする場合の接点スパークなど)を発生する装置の近く(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください)。

本体をラックに取り付ける手順を以下に示します。取り外し手順については、取り付け手順の後で説明しています。
ここでは、NEC製のラックまたは他社製ラックへの取り付け手順について説明します。
NEC製のラックのうち、N8540-28/29/38に取り付ける場合は、オプションの「N8143-35 ラック取り付け用ブラケット」が必要です。取り付け手順については、N8143-35 ラック取り付け用ブラケットに添付の説明書を参照するか、保守サービス会社にお問い合わせください。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **規格外のラックで使用しない**
- **指定以外の場所で使用しない**

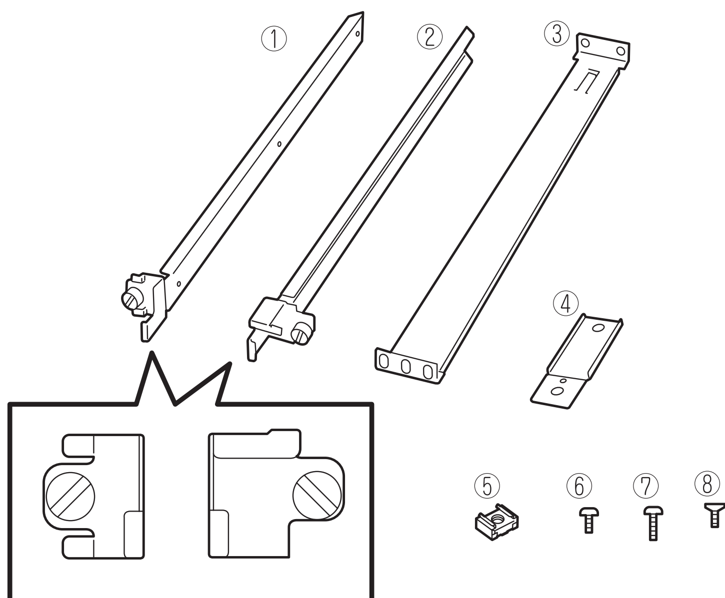
⚠注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **落下注意**
- **装置を引き出した状態にしない**
- **カバーを外したまま取り付けない**
- **指を挟まない**

取り付け部品の確認

ラックへ取り付けるために次の部品があることを確認してください。



項番	名称	数量	備考
①	マウントブラケット(L)	1	「L」と刻印されている。
②	マウントブラケット(R)	1	「R」と刻印されている。
③	サポートブラケット	2	
④	エクステンションブラケット	2	
⑤	コアナット	8	
⑥	ネジA	4	M3ネジ、ネジ部の長さ: 5mm、マウントブラケット(L)/(R)を装置に固定する際に使用する。
⑦	ネジB	6	M5ネジ、ネジ部の長さ: 10mm、サポートブラケットを固定する際に使用する。
⑧	ネジC	2	皿ネジ、エクステンションブラケットを固定する際に使用する。

必要な工具

ラックへ取り付けるために必要な工具はプラスドライバとマイナスドライバです。

取り付け手順

次の手順で本体をラックに取り付けます。



NEC製のラックのうち、N8540-28/29/38への取り付けにはN8143-35 ラック取り付け用ブラケットが必要となります。また、取り付け方法についてはN8143-35 ラック取り付け用ブラケットに添付の説明書をご覧ください。

● マウントブラケットの取り付け

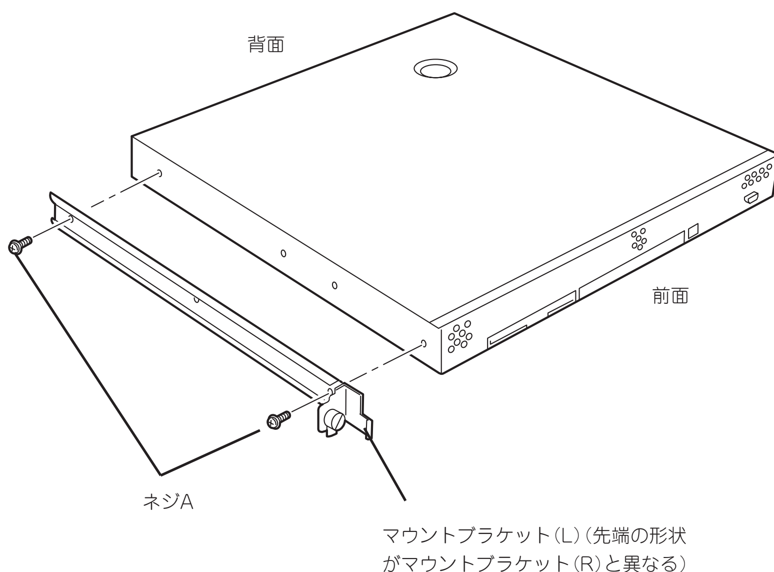
1. マウントブラケットのネジ穴と本体側面のネジ穴を合わせる。



ブラケットの向きを確認して取り付けてください。本体左側面にマウントブラケット(L)、右側面にマウントブラケット(R)を取り付けます。それぞれのブラケットに「L」、「R」と刻印があります。

2. マウントブラケットをネジA(2本)で本体に固定する。

3. もう一方の側面にマウントブラケットを手順1〜2と同じ手順で取り付ける。

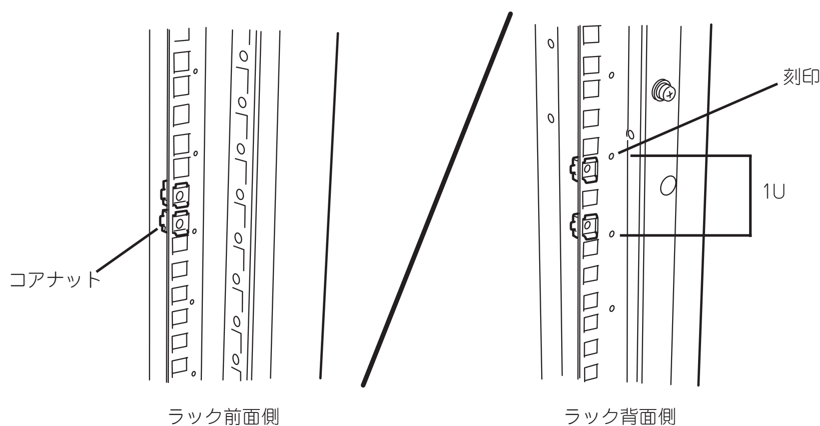


- **コアナットの取り付け**

サポートブラケットを固定する位置に本装置に添付のコアナットを取り付けます。コアナットはラックの前面（左右とも）に各2個、背面（左右とも）に各2個の合計8個取り付けます。

コアナットは「1U（ラックでの高さを表す単位）」の中に2個取り付けてください（NEC製のラックでは、1U単位に丸い刻印があります）。1Uあたり、スロット（角穴）が3つあります。3つのスロットのうち、ラック前面側では下の2つのスロットに、ラック背面側では上下のスロットにコアナットを取り付けます。

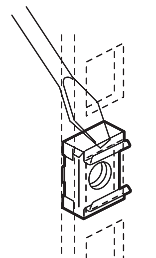
コアナットはラックの内側から取り付けます。ラックの前面に取り付けたコアナットは、上側が本体のセットスクリューの受けとなります。下側はサポートブラケット前面の固定に使用します。背面のコアナットはサポートブラケット背面の固定用として使われます。



コアナットは下側のクリップをラックの四角穴に引っかけてからマイナスドライバなどで上側のクリップを穴に差し込みます。

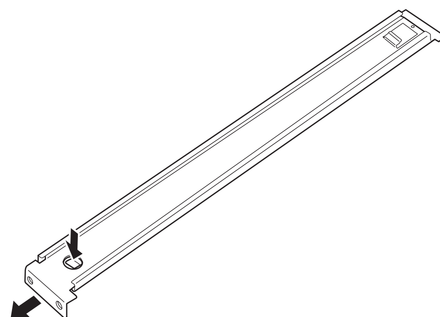


ラックの前後、左右に取り付けたコアナットの高さが同じであることを確認してください。



● サポートブラケットの取り付け

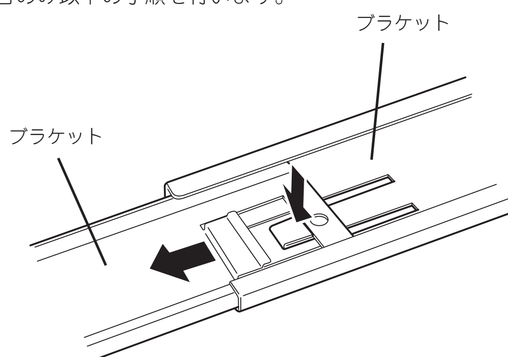
1. サポートブラケットのロックを解除して引き延ばす。



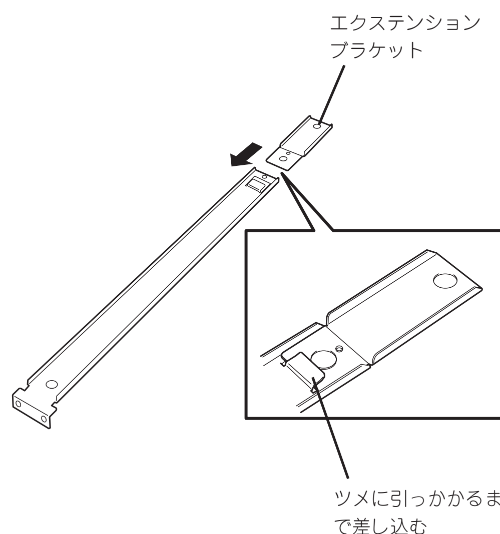
2. <ラックの前後の奥行きが700mm以上の場合のみ>

   ラックの前後の奥行きが700mm以上の場合のみ以下の手順を行います。

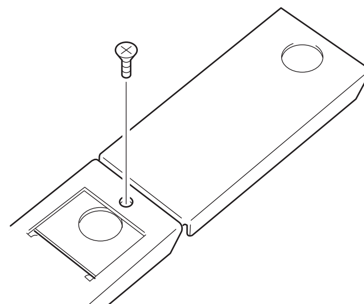
   ① サポートブラケットのロックを解除してブラケットを分解する。



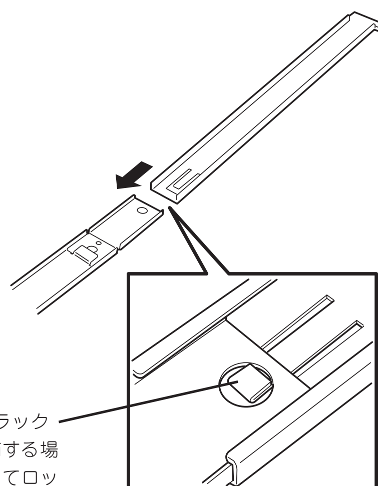
   ② エクステンションブラケットを一方のブラケットに差し込む。



③ エクステンションブラケットをネジC(1本)で固定する。



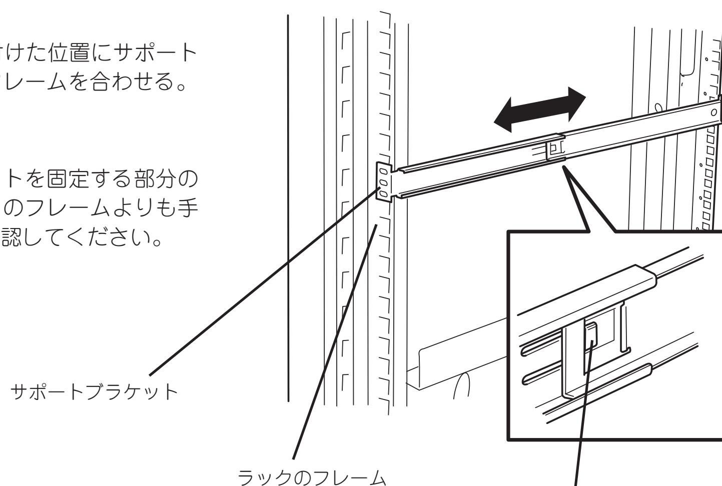
④ もう一方のブラケットをエクステンションブラケットに差し込む。



3. コアナットを取り付けた位置にサポートブラケット前後のフレームを合わせる。



サポートブラケットを固定する部分のフレームがラックのフレームよりも手前にあることを確認してください。



4. サポートブラケットを支えながら、ネジB(3本)でラックに固定する。



サポートブラケットが水平に取り付けられていることを確認してください。

本体のセットスクリューの受けに使用する

ネジB

ラック前面側

ラック背面側



サポートブラケットのネジ穴は多少上下にずらすことができる程度のクリアランスを持っています。初めて取り付ける場合は、コアナットのネジ穴がサポートブラケットのネジ穴の中央に位置するようにしてから固定してください。もし、装置を取り付けたときに装置の上下に搭載している装置にぶつかる場合は、いったん本装置を取り出してサポートブラケットの固定位置を調整してください(ぶつかる装置の取り付け位置も調整する必要がある場合もあります)。

5. もう一方のサポートブラケットを手順1〜4と同じ手順で取り付ける。



すでに取り付けているサポートブラケットと同じ高さに取り付けていることを確認してください。

● 本体の取り付け

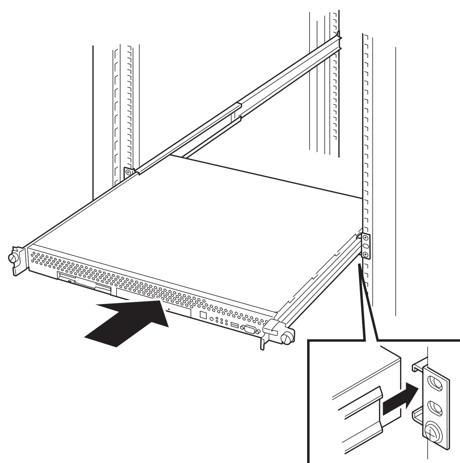
取り付けは1人でもできますが、なるべく複数名で行うことをお勧めします。

1. 本体前面が手前になるようにして持つ。

2. 本体側面に取り付けたマウントブラケットをサポートブラケットに差し込みながらラックへ押し込む。

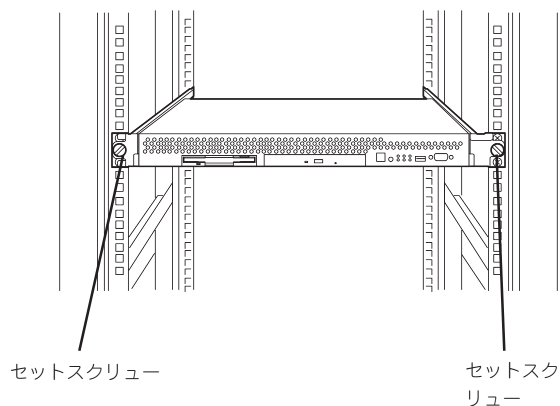


装置の上下に搭載している装置にぶつかる場合は、いったん本装置を取り出してサポートブラケットの固定位置を調整してください。(ぶつかる装置の取り付け位置も調整する必要がある場合もあります)。

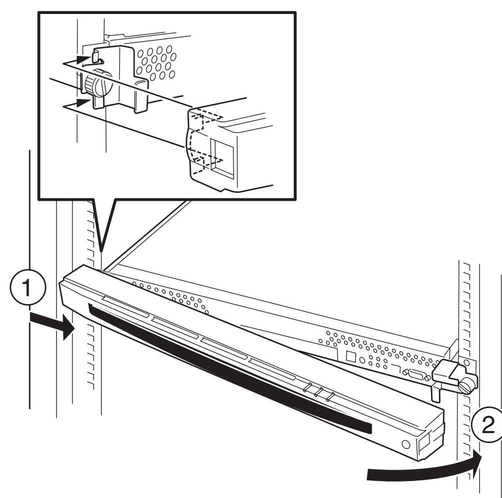


● 本体の固定

1. 本体をラックへ完全に押し込む。

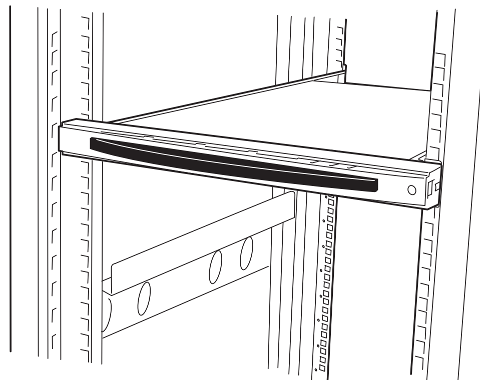


2. 前面の左右にあるセットスクリューでラックに固定する。



3. フロントベゼルを取り付ける。

以上で完了です。



取り外し手順

次の手順で本体をラックから取り外します。取り外しは1人でもできますが、なるべく複数名で行うことをお勧めします。

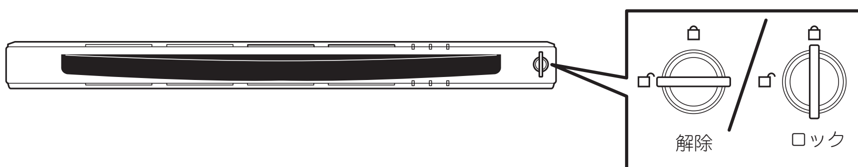
⚠注意



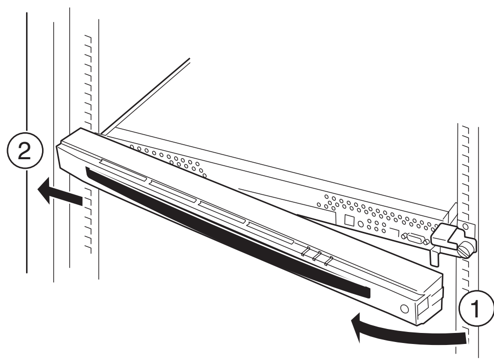
装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 指を挟まない
- ラックが不安定な状態でデバイスをラックから引き出さない
- 落下注意
- 装置を引き出した状態にしない
- 複数台のデバイスをラックから引き出した状態にしない
- 動作中に装置をラックから引き出さない

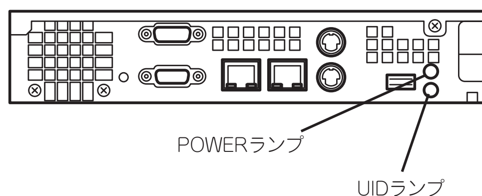
1. フロントベゼルのロックを解除する。



2. フロントベゼルを取り外す。
3. 本体の電源をOFF（POWERランプ消灯）にする。



4. 本体前面にあるUIDスイッチを押して、UIDランプを点灯させる。
5. 本体に接続しているすべてのケーブル、および電源コードを取り外し、UIDランプが消灯していることを確認する。



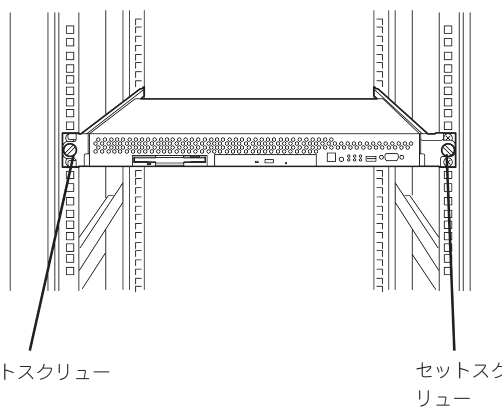
> ✔ チェック
>
> 本体背面のケーブルや電源コードを取り外す前にUIDランプで取り外そうとしている装置であることを確認してください。

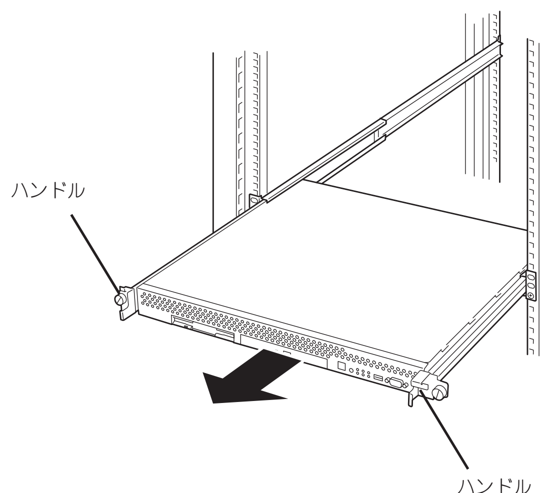
6. 前面の左右にあるセットスクリューをゆるめて、ハンドルを持ってゆっくりとラックから引き出す。

本体の両端をしっかりと持てる位置(約15cmほど)までゆっくりと静かにラックから引き出してください。

重要

装置を引き出しすぎると、サポートブラケットから装置が外れて落下するおそれがあります。





7. 本体の左右底面をしっかりと持って取り外し、じょうぶで平らな机の上に置く。

重要

装置を引き出したまま放置しないでください。必ずラックから取り外してください。

ラックの機構部品も取り外す場合は、「取り付け手順」を参照して取り外してください。

接　続

本体をネットワークに接続します。
ネットワークケーブルを本体に接続してから添付の電源コードを本体に接続し、電源プラグをコンセントにつなげます。

警告



装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- ぬれた手で電源プラグを持たない
- アース線をガス管につながない

注意



装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

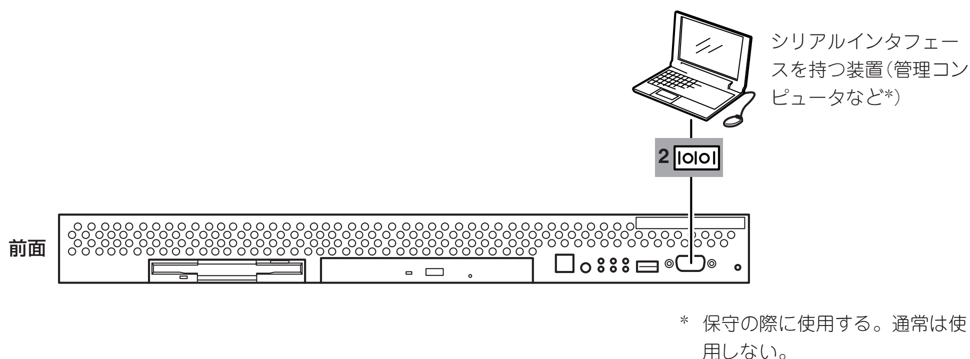
- 指定以外のコンセントに差し込まない
- たこ足配線にしない
- 中途半端に差し込まない
- 指定以外の電源コードを使わない
- プラグを差し込んだままインタフェースケーブルの取り付けや取り外しをしない
- 指定以外のインタフェースケーブルを使用しない

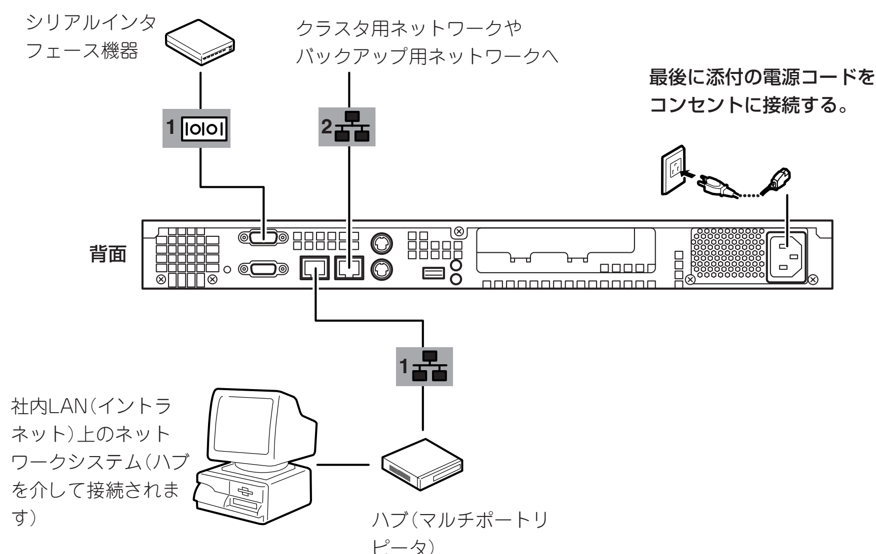


- 本体および接続する周辺機器の電源をOFFにしてから接続してください。ONの状態のまま接続すると誤動作や故障の原因となります。
- NEC以外(サードパーティ)の周辺機器およびインタフェースケーブルを接続する場合は、お買い求めの販売店でそれらの装置が本装置で使用できることをあらかじめ確認してください。サードパーティの装置の中には本装置で使用できないものがあります。



無停電電源装置(UPS)を導入し、電源制御システムの構築を検討されている場合は、お買い求めの販売店または保守サービス会社にお問い合わせください







ネットワークに接続する前に次の点について確認してください。

- LANのネットワーク設定

  本装置に割り当てるIPアドレスやネットワーク環境について確認してください。

- ネットワーク機器

  必要なルータ、ハブ、ケーブルが準備されていることを確認してください。また ISPとの接続に用いるルータもしくはダイヤルアップルータに、あらかじめインターネット接続に必要な設定を行い設置しておいてください(イントラネットで用いる場合は必要ないこともあります)。

- クライアントPC

  本装置とは別に、Windows 2000、Windows NT、またはWindows Me/98/95のいずれかのWindows OSが利用可能なクライアントマシン(PC)を用意してください。最低限の初期設定を行うための「初期導入設定ツール」の実行に利用します。

以上で本体の電源をONにできる状態になりました。購入後、初めて本体の電源をONにする場合は、この後の「初めてのセットアップ」をご覧ください。再セットアップの場合は、55ページの「再セットアップ」を参照してください。

初めてのセットアップ

購入後、初めてシステムをセットアップする時の手順について順を追って説明します。

初期導入設定用ディスクの作成

「初期導入設定用ディスク」は装置を導入するために最低限必要となる設定情報が保存されたセットアップ用のフロッピーディスクです。

「初期導入設定用ディスク」は、添付の初期導入設定用ディスクにある「初期導入設定ツール」を使って作成します。初期導入設定ツールは、Windows 2000、Windows NT、またはWindows Me/98/95で動作するコンピュータで動作します。

初期導入設定プログラムの実行と操作の流れ

Windowsマシンを起動して、次の手順に従って初期導入設定用ディスクを作成します。

1. Windowsマシンのフロッピーディスクドライブに添付の初期導入設定用ディスクをセットする。
2. フロッピーディスクドライブ内の「初期導入設定ツール(startupConf.exe)」をエクスプローラなどから実行する。

   [Linuxビルドアップサーバ初期導入設定ツール]が起動します。プログラムは、ウィザード形式となっており、各ページで設定に必要事項を入力して進んでいきます。

   必須情報が入力されていない場合や入力情報に誤りがある場合は、次へ進むときに警告メッセージが表示されます。項目を正しく入力し直してください。入力事項については、この後の説明を参照してください。

   すべての項目の入力が完了すると、フロッピーディスクに設定情報を書き込んで終了します。
3. 初期導入設定用ディスクをフロッピーディスクドライブから取り出し、「システムのセットアップ」に進む。

   初期導入設定用ディスクは再セットアップの際にも使用します。大切に保管してください。

各入力項目の設定

[Linuxビルドアップサーバ初期導入設定ツール]で入力する項目について説明します。

パスワード設定

システムのセットアップ完了後、管理コンピュータからWebブラウザを介して、システムにログインする際のパスワードを設定します。この画面にある項目はすべて入力しないといけません。
パスワードは推測されにくく覚えやすいものを用意してください。

チェック

パスワードは画面に表示されません。タイプミスをしないよう注意してください。

設定済みパスワード

初めて設定する場合は、同梱の別紙「rootパスワード」に記載されたパスワードを入力してください。以前に設定を行っている場合は、設定されているパスワードを入力してください。

パスワード

設定するパスワードを入力してください。ここで入力したパスワードは、管理者(admin)でログインする場合に必要となります。パスワードを忘れたり、不正に利用されたりしないように、パスワードの管理は厳重に行ってください。

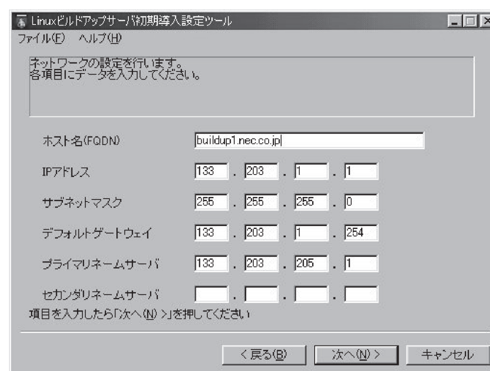
なお、パスワードを変更したくない場合は、既存パスワードと同一のパスワードを新パスワードとして設定してください。

パスワード再入力

パスワードの確認用です。パスワードと同一のものを入力してください。

ネットワーク設定　～LANポート1(標準LAN)用～

LANポート1(標準LAN)のネットワーク設定をします。[セカンダリネームサーバ]以外は必ず入力してください。



ホスト名(FQDN)

ホスト名を入力してください。入力の際には、FQDNの形式 (マシン名.ドメイン名)の形式で入力してください。また、英字はすべて小文字で指定してください。大文字は使用できません。

IPアドレス

1枚目のNIC(LANポート1(標準LAN))に割り振るIPアドレスを指定してください。

サブネットマスク

1枚目のNIC(LANポート1(標準LAN))に割り振るサブネットマスクを指定します。

ディフォルトゲートウェイ

ディフォルトゲートウェイのIPアドレスを指定します。

プライマリネームサーバ

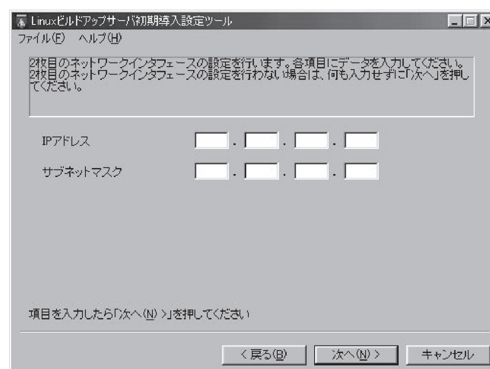
プライマリネームサーバのIPアドレスを指定します。

セカンダリネームサーバ

セカンダリネームサーバが存在する場合は、そのIPアドレスを指定します。

ネットワーク設定　～LANポート2(拡張LAN)用～

LANポート2(拡張LAN)のネットワーク設定をします。使用しない場合は、設定する必要はありません。



IPアドレス

2枚目のNIC(LANポート2(拡張LAN))に割り振るIPアドレスを指定してください。

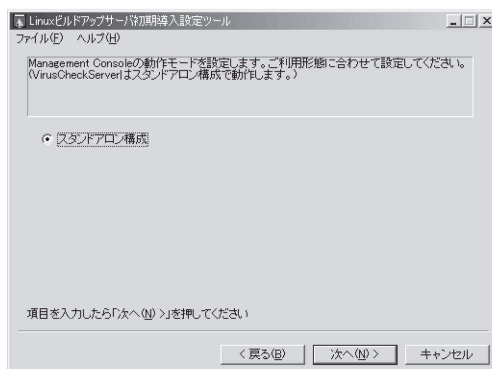
サブネットマスク

2枚目のNIC(LANポート2(拡張LAN))に割り振るサブネットマスクを指定します。

システム構成条件の設定

Management Consoleの動作モードを設定します。

VirusCheckServerは[スタンドアロン構成]で動作します。



システムのセットアップ

初期導入設定ツールで作成した「初期導入設定用ディスク」を使用して、短時間でセットアップできます。

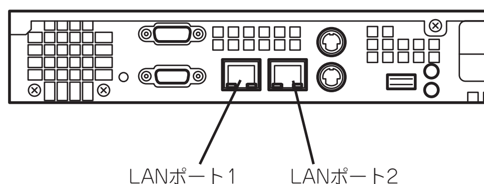
セットアップの手順

以下手順でセットアップをします。

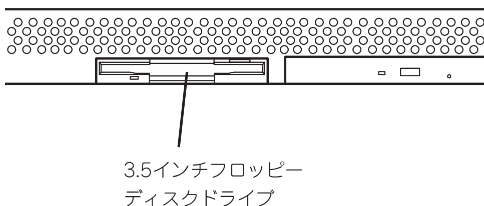


正しくセットアップできないときは、次ページ、および176ページを参照してください。

1. 本体背面のLANポート1とLANポート2（使用する場合）にネットワークケーブルが接続されていることを確認する。



2. 前述の「初期導入設定用ディスクの作成」で作成した初期導入設定用ディスクを3.5インチフロッピーディスクドライブにセットする。

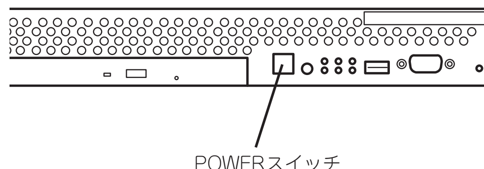


3. POWERスイッチを押す。

POWERランプが点灯します。

しばらくすると、初期導入設定用ディスクから設定情報を読み取り、自動的にセットアップを進めます。2〜3分ほどでセットアップが完了します。

次項および3章を参照してシステムの状態確認や設定変更を行ってください。



重要

セットアップの完了が確認できたらセットした初期導入設定用ディスクをフロッピーディスクドライブから取り出して大切に保管してください。再セットアップの時に再利用することができます。

セットアップに失敗した場合

システムのセットアップに失敗した場合は、ビープ音をらすことでユーザーに異常を知らせます(自動的に電源がOFF(POWERランプ消灯)になります)。正常にセットアップが完了しなかった場合は、初期導入設定用ディスクに書き出されるログファイル「logging.txt」の内容をコンピュータの「メモ帳」などのツールを使って確認し、再度初期導入設定ツールを使用して初期導入設定用ディスクを作成し直してください。

<主なログの出力例>

■ 「Info: completed.」

→ 正常にセットアップが完了した場合に表示されます。

■ 「Info: quitting with no change.」

→ 初期導入設定ツールを使って再度作成せずに、一度セットアップに使用した初期導入設定用ディスクを再使用した場合に表示されます(設定は反映されません)。

■ 「Cannot get authentication: root」

→ 初期導入設定用ディスク中のパスワードの指定に誤りがある場合に表示されます。

■ 「Error: invalid file: /mnt/floppy/linux.aut」

→ 初期導入設定用ディスク中のパスワード情報を格納したファイル(linux.aut)が正しく作成されなかった場合に表示されます。

■ 「Error: cannot open: /mnt/floppy/linux.aut」

→ 初期導入設定用ディスク中のパスワード情報を格納したファイル(linux.aut)が正しく作成されなかった場合に表示されます。

セットアップや運用時のトラブルについての対処を174ページで詳しく説明しています。

セットアップの確認

インストールされているInterScan VirusWallは初期設定値に従って動作するように設定されていますが、パターンの配信サーバへの登録など少なくとも1回はInterScanコンソールを開き、設定内容を確認するようにしてください。



InterScan VirusWallの詳細な設定は基本ライセンスに添付の「InterScan VirusWall管理者ガイド」を参照してください。

1. InterScanコンソールを開く。

   InterScanコンソールを開くには次の2つの方法があります。

   - Management Consoleからサービスのアイコンを選択し、[ウイルスチェック]をクリックする。
   - Webブラウザを起動し、ポート番号(:1812)を付けたInterScanのURLを入力する。

     IPアドレスの部分は、 InterScanマシンのドメイン名、 IPアドレスのいずれでもかまいません。次に例を示します。

     http://ドメイン名:ポート/interscan
     http://isvw.widget.com:1812/interscan
     http://123.12.123.123:1812/interscan

2. InterScanコンソールにログインするためのユーザ名とパスワードを入力する。

   InterScanコンソールにはパスワードが設定されています。初期設定では、ユーザ名、パスワードともに adminが設定されています。

   以降の各設定ページで項目を変更した際には、[Apply]ボタンをクリックして、設定を保存してください。

   [Apply]ボタンをクリックせずにブラウザを終了したり、他のページを表示すると、変更が取り消されます。[Cancel]ボタンをクリックすると、各項目は設定変更前の値に戻ります。

ウイルスパターンファイル

ウイルスを検出するために、InterScan VirusWallでは、一般にウイルスパターンファイルと呼ばれる、ウイルスシグネチャの大規模なデータベースを利用しています。新しいウイルスが作成され、世間に送り出され、検出されると、トレンドマイクロ社ではそのシグネチャを収集して、ウイルスパターンファイルに情報を追加します。ウイルスパターンファイルの命名規則は次のとおりです。

lpt$vpn.###

###は、バージョン番号(たとえば505)を表します。同じディレクトリに複数のファイルが存在する場合、最も大きな番号のファイルのみが使用されます。
トレンドマイクロ社では、ほぼ毎週新しいウイルスパターンファイルを提供していますので、少なくとも数週間ごとにパターンファイルをアップデートするようにしてください。登録ユーザは、無料でアップデートファイルを入手できます。アップデートファイルは、インターネット経由で自動的にダウンロードすることができます。



古いパターンファイルを削除する必要はなく、また新しいファイルを使用するために、特別なインストール手順を実行する必要はありません。後述の[Update Virus Pattern Now]ボタンをクリックするだけで、システムが自動的に新しいパターンファイルを設定します。

ウイルスパターンファイルを手動でアップデートする

ウイルスパターンファイルを手動でアップデートするには、次の手順に従ってください。

1. InterScanコンソールを開き、[Pattern Update]をクリックする。

   画面には現在のパターンファイルのバージョンと、前回のアップデート日時が表示されています。

   ウイルスパターンアップデートのためのユーザ登録を実行していない場合には、ウイルスパターンファイルをアップデートする前に、[Register for Virus Pattern Updates]画面からユーザ登録を実行してください。

2. [Update Virus Pattern Now]ボタンをクリックする。

   トレンドマイクロ社の提供するパターンファイルがInterScanサーバ上のファイルよりも新しい場合にのみ、アップデートが実行されます。

ウイルスパターンファイルを自動アップデートを設定する

自動アップデートを設定するには、次の手順に従ってください。

1. InterScanコンソールを開き、[Pattern Update]をクリックする。
2. [Set Automatic Update Time]をクリックする。

   自動アップデートのためのオプションを設定する[Set Automatic Update Time]画面が表示されます。

3. **<ウイルスパターンファイルの自動アップデートを無効にする場合>**

   [No automatic update]を選択する。

   <ウイルスパターンファイルの自動アップデートを実行する場合>

   必要に応じて周期オプションを選択する。
   また、必要に応じて、[Start time]でアップデートを実行する時刻を選択してください。

HTTPプロキシサーバの使用

InterScanでは、インターネット上のトレンドマイクロ社のサイトから、新しいウイルスパターンファイルを取得します。InterScanとインターネットの間に HTTPプロキシサーバが設定されている環境で、このサイトにアクセスする場合には、HTTPプロキシサーバを指定して、プロキシサーバにログオンするための情報を指定する必要があります。



Trend Virus Control System(以降、「Trend VCS」と省略します)エージェントはTrend VCS サーバにアクセスする際に、同じプロキシサーバ情報を使用します。

プロキシサーバを指定するには、次の手順に従ってください。

1. InterScanコンソールを開き、[Pattern Update]をクリックする。
2. [Set Proxy Server]をクリックする。

   [Set Proxy for Update Virus Pattern From Internet]画面が表示されます。

3. InterScanとインターネットの間にプロキシサーバが存在する場合は、[Use proxy server for pattern download]を選択する。

   プロキシサーバが存在しない場合は、初期設定のまま[Do not use proxy server for pattern download]をチェックしておく。

   a. [proxy]に、プロキシサーバのドメイン名(またはIPアドレス)を入力します(例: proxy.company.com)。

   b. [port]にプロキシサーバが使用するポート番号を入力します(例: 80または8080)。

4. プロキシサーバにログインする際に InterScanが使用するユーザIDとパスワードを、それぞれ[User ID]、[Password]に入力する。

検索エンジンのアップデート

トレンドマイクロ社では継続的にInterScanの検索エンジンを見直し、新しい機能や機能改善を追加しています。更新された検索エンジンは、トレンドマイクロ社のダウンロードサイトに登録されます。検索エンジンを自動的にアップデートすることはできません。検索エンジンをアップデートする場合は、以下のURLから検索エンジンをダウンロードし、/etc/iscanディレクトリにコピーしてください。

http://www.trendmicro.co.jp

InterScan VirusWallのユーザー登録

ユーザー登録は非常に大切な作業であり、InterScan VirusWallのユーザー登録を行うと、次のサービスを受けることができます。

- 1年間の無料ウイルスパターンファイルのアップデート
- 1年間の無料サポートサービス
- 製品の更新情報や新製品案内のご提供

ソフトウェアは次の方法で登録できます。

- インターネット経由の登録
- FAXによる登録

インターネット経由のユーザー登録は、非常に高速また便利な方法です。必要な情報を入力して[Register]をクリックしてデータをトレンドマイクロ社に送信するだけで、ウイルスパターンファイルのアップデートのサービスを受けられるようになります。
サポートサービスや情報提供はサポート申し込み書による登録が必要です。



InterScanとインターネットの間にHTTPプロキシサーバが設定されている場合には、InterScan VirusWallでHTTPプロキシサーバを設定する必要があります。詳細については、「HTTPプロキシサーバの使用」を参照してください。

インターネット経由でユーザー登録するには、次の手順に従ってください。

1. Webブラウザを起動して、 InterScanコンソールを開き、ブラウザの左側のフレームで、[Pattern Update]をクリックする。
2. [Update Virus Pattern From Internet]ページで、[Register for Virus Pattern Update]をクリックする。

   [Register For Virus Pattern Updates]画面が表示されます。
3. 必要事項をすべて記入する。

   基本ライセンスに添付されているシリアル番号を入力してください。
4. [Register]をクリックして、入力した情報をトレンドマイクロ社に送信する。

   プログラムからウイルスパターンファイルのアップデートを受信するには、インターネット経由でユーザー登録を実行する必要があります。

E-Mail VirusWallの設定

E-Mail VirusWallは、お使いのネットワーク環境に応じて、さまざまな設定でご利用いただくことができます。
詳細については、基本ライセンスに添付の「InterScan VirusWall管理者ガイド」を参照してください。



[E-Mail Scan Configuraiont]ページの[Main service port]の設定は、E-Mail VirusWallを導入する際のトポロジに依存します。
トポロジの詳細については、管理者ガイドの第2章を参照してください。

ローカルホスト上のsendmailを使用する場合

1. InterScan設定ページを表示し、[Configuration]→[E-Mail Scan]を選択する。
2. [Original SMTP server location]で[Local server]を選択する。
3. オリジナルの sendmailを指定する。

   <コマンドモードの場合>

   [Command mode]を選択し、ローカルホスト上の sendmail プログラムのパスを指定します。必要であればパラメータも指定します(例: /usr/lib/sendmail -bs)。

   <デーモンモードの場合>

   [Daemon mode]を選択し、[Port Number]にオリジナルの sendmailで使用するポート番号を指定します。

リモートサーバ上のSMTPサーバを使用する場合

1. InterScan 設定ページを表示し、[Configuration]→[E-Mail Scan]を選択する。
2. [Original SMTP server location]で[Remote server]を選択する。
3. オリジナルのSMTPサーバを指定する。

   [Hostname]にオリジナルのSMTPサーバが動作するリモートサーバのサーバ名またはIPアドレスを指定します(例: remoce.com)。
   [Port number]にオリジナルのSMTPサーバが使用するポート番号を指定します。ポート番号には、ほとんどの場合、25を指定します。
   次に例を示します。

   mailserver 25
   mailserver.yourcompany.com 25
   123.12.12.123 25

InterScan VirusWallの動作

E-Mail VirusWallは、ポート番号25でSMTPトラフィックを受信後、対象となるトラフィックのウイルスを検索し、指定されたポート(ここでは25)を使用して、[Original SMTP server location]で指定された SMTPサーバにルーティングします。

Web VirusWallの設定

Web VirusWall は、お使いのシステムの設定に従って独自のプロキシサーバとして設定することも、既存の HTTPプロキシサーバと併用することもできます。システムの設定に応じて、 InterScanコンソールの[HTTP Scan Configuration]ページで、[InterScan acts as a proxy itself]または[Other (server and port)]のどちらかを選択し、[InterScan HTTP Proxy port (connects to browser)]にポート番号(通常は80)を指定します。



Web VirusWallでFTPトラフィックを検索する場合は、クライアント側のWebブラウザで、Web VirusWallをFTPプロキシとして使用するように設定する必要があります。

オリジナル HTTPサーバの指定: [Original HTTP server location]

1. 管理コンソールで[Configuration]→[HTTP Scan]を選択し、[InterScan HTTP Proxy port...]に、Web VirusWallがクライアントからの接続を監視するポート番号を入力する。

   通常は80を指定します。

2. [Original HTTP server location]で、[InterScan acts as a proxy itself]、または[Other (server and port)]を選択して、サーバ名(または IPアドレス)とポート番号を指定する。

   [InterScan acts as a proxy itself]

   ネットワーク上に既存の HTTPプロキシサーバがなく、Web VirusWallをシステム全体のHTTPプロキシサーバとして使用する場合、または Web VirusWallを論理上インターネットとプロキシサーバの間に配置する場合には、このオプションを選択します。

   [Other (server and port)]

   ネットワーク上に既存のHTTPサーバがある場合には、このオプションを選択し、サーバ名とポート番号を入力します。Web VirusWallでは、ここで指定されたマシンに対するすべてのHTTPトラフィック、およびそのマシンからのすべてのHTTPトラフィックについて、ウイルス検索を行います。

3. [Other (server and port)]に、 HTTP デーモン(in.httpd)を実行するマシンのドメイン名またはIPアドレスを入力します。次に例を示します。

   proxy.yourcompany.com 80
   123.12.13.123 80

テスト

Telnetまたは同様のプログラムを使用して、上記の設定で指定したInterScanのIPアドレスおよびポート番号に対して、Telnetを実行します。サーバからの応答の内容を確認することで、ほとんどの設定を識別し、解決することができます。

FTP VirusWallの設定

[FTP Scan Configuration]ページで指定する FTPサーバの場所とポート番号は、FTP VirusWallが独自のプロキシサーバとして導入されるかどうか、既存のFTPサーバと併用するように導入されるかどうか、などに依存します。

オリジナル FTP サーバの指定: [Original FTP server location]

1. 管理コンソールで[Configuration] →[FTP Scan]を選択する。

2. [Main service port]にFTP VirusWallでクライアントからの新しい接続を監視するポートの番号を指定する。

   通常は21を指定します。

3. [Use user@host]または[Server location]のいずれかを選択する。

   [Server location]を選択した場合は、FTPサーバのパスとポート番号を設定してください。

   [Use user@host]: ネットワークで唯一の FTPサーバとして動作する場合

   FTP VirusWallをシステムのFTPサーバとして使用する場合は、[Use user@host]を選択してください。クライアントからは常にInterScanにFTP接続し、InterScanでは要求されたサイトに対する接続を確立します。クライアントでユーザ名とパスワードの入力が要求された際に、ユーザ名に対象となるドメインのドメイン名をつけることを忘れないでください。たとえば、ユーザjohnがwidgets.comにFTP接続する場合の例を示します。

   – widgets.comに直接接続する場合

     ユーザ名: john
     パスワード: opensesame

   – FTP VirusWallを介して接続する場合

     ユーザ名: john@widgets.com
     パスワード: opensesame

   [Server location]: ネットワーク上に既存の FTP サーバがある場合

   ネットワーク上に既存のFTPサーバがある場合には、[Server location]を選択し、テキストボックスにサーバのパスとポートを入力します。FTP VirusWallでは、ここで指定されたマシンに対するすべてのFTPトラフィック、およびそのマシンからのすべてのFTPトラフィックについて、ウイルス検索を実行します。

4. [Original FTP server location]の[Server location]に、既存のFTPサーバのホスト名(またはIPアドレス)とポート番号を入力する。

   次に例を示します。

   ftp-server.yourcompany.com 21
   123.12.13.123 21

テスト

Telnetまたは同様のプログラムを使用して、前述の設定で指定した InterScanのIPアドレスおよびポート番号に対して、Telnetを実行します。サーバからの応答の内容を確認することで、ほとんどの設定を識別し、解決することができます。

ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。5章を参照してセットアップしてください。

システム情報のバックアップ

システムのセットアップが終了した後、添付の「保守・管理ツールCD-ROM」にあるオフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。



保守・管理ツールCD-ROMからシステムを起動して操作します。保守・管理ツールCD-ROMから起動させるためには、事前にセットアップが必要です。4章を参照して準備してください。

1. 3.5インチフロッピーディスクを用意する。
2. 本体に添付の「保守・管理ツールCD-ROM」から「オフライン保守ユーティリティ」を起動する。

   「保守・管理ツールCD-ROM」の使い方については4章を参照してください。
3. [システム情報の管理]から[退避]を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

続いて管理コンピュータに本装置を監視・管理するアプリケーションをインストールします。次ページを参照してください。

セキュリティパッチの適用

最新のセキュリティパッチは、以下のURLよりダウンロード可能です。

http://www.express.nec.co.jp/care/index.asp

定期的に参照し、適用することをお勧めします。

管理コンピュータのセットアップ

本装置をネットワーク上のコンピュータから管理・監視するためのアプリケーションとして、「ESMPRO/ServerManager」と「Management Workstation Application（MWA）」が用意されています。
これらのアプリケーションを管理コンピュータにインストールすることによりシステムの管理が容易になるだけでなく、システム全体の信頼性を向上することができます。

ESMPRO/ServerManagerのインストールについては5章を参照してセットアップしてください。

MWAのインストールについては4章、または保守・管理ツールCD-ROM内のオンラインドキュメントを参照してください。

再セットアップ

再セットアップとは、システムクラッシュなどの原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

保守用パーティションの作成

「保守用パーティション」とは、装置の維持・管理を行うためのユーティリティを格納するためのパーティションで、16MB程度の領域を内蔵ハードディスク上へ確保します。
システムの信頼性を向上するためにも保守用パーティションを作成することをお勧めします。保守用パーティションは、添付の「保守・管理ツールCD-ROM」を使って作成します。詳しくは第4章を参照してください。
保守用パーティションを作成するプロセスで保守用パーティションへ自動的にインストールされるユーティリティは、「システム診断ユーティリティ」と「オフライン保守ユーティリティ」です。

再セットアップモードへの変更

本装置は、システムの起動が正常に行われたかどうか常に監視をし、起動に失敗した場合はシステムの再起動を試みる機能が備わっています。再インストール中は、システム起動監視機能を無効にする必要があります。
本機能の有効／無効は、添付の「保守・管理ツールCD-ROM」を使って変更します。詳しくは、4章を参照してください。



再セットアップが完了したら、システム起動監視機能を有効に戻してください。

システムの再インストール



再インストールを行うと、サーバ内の全データが消去され、出荷時の状態に戻ります。必要なデータがサーバ内に残っている場合、データをバックアップしてから再インストールを実行してください。

再インストールには、本体添付のバックアップCD-ROMとバックアップCD-ROM用インストールディスクが必要です。
「バックアップCD-ROM用インストールディスク」を3.5インチフロッピーディスクドライブに、「バックアップCD-ROM」をCD-ROMドライブにそれぞれ挿入し、POWERスイッチを押して電源をONにします。



このとき、前面のシリアルポート2(COM2)に管理コンピュータを19,200bpsの転送速度で接続すると、管理コンピュータからログを参照することができます。

しばらくすると「バックアップCD-ROM用インストールディスク」から設定情報を読み取り、自動的にインストールを実行します。



このとき、確認等は一切行われずにインストール作業が開始されるため、十分注意してください。

約30分程度でインストールが完了します。インストールが完了したら、CD-ROMが自動的にイジェクトされます。CD-ROMとフロッピーディスクの両方をドライブから取り出してください。

40分以上待っても、CD-ROMがイジェクトされず、CD-ROMへのアクセスも行われていない場合は再インストールに失敗している可能性があります。リセットして、CD-ROM/フロッピーディスクをセットし直して再度インストールを試みてください。それでもインストールできない場合は、保守サービス会社、またはお買い上げの販売店までご連絡ください。

初期導入設定用ディスクの作成

前述の「初期導入設定用ディスクの作成」を参照してください。すでに初期導入設定用ディスクを作成している場合は、パスワード情報の設定のみ再度設定し直してください。ただし、設定内容を変えたいときは、新たに初期導入用設定ディスクを作り直してください。

システムのセットアップと確認

前述の「システムのセットアップ」、「セットアップの確認」を参照してください。

ESMPRO/ServerAgentのセットアップ

「システムの再インストール」でESMPRO/ServerAgentは自動的にインストールされますが、固有の設定がされていません。5章を参照してセットアップしてください。

セキュリティパッチの適用

最新のセキュリティパッチは、以下のURLよりダウンロード可能です。

http://www.express.nec.co.jp/care/index.asp

定期的に参照し、適用することをお勧めします。